IN THE CLAIMS:

1. CANCEL.

2. (Currently Amended) The method of claim 4 ~~claim 1~~, wherein the guard message employs a smart message implemented as a bearer-independent object, or employs wireless access protocol push messaging.

3. (Currently Amended) The method of claim 4 ~~claim 1~~, wherein the guard message employs synchronization markup language device management.

4. (Currently Amended) A method ~~for increasing security of a mobile terminal that has been lost, stolen, or misplaced by a user~~, comprising:

inputting a personal identification code, at a location separate from a mobile terminal that has been lost, stolen, or misplaced,

sending the personal identification code via a telephone connection to an automated or human attendant,

receiving the personal identification code and using the personal identification code to determine from a database whether the mobile terminal has a device management feature supporting synchronization markup language,

composing a guard message that employs synchronization markup language if the mobile terminal has the device management feature,

composing the guard message so that the guard message instead employs a smart message implemented as a bearer-independent object or employs wireless access protocol push messaging, if the mobile terminal lacks the device management feature,

~~receiving~~ sending the guard message ~~a guard message at the~~ from the attendant to the mobile terminal,

authenticating the guard message at the mobile terminal,

locking at least one communication capability of the mobile terminal, and

securing at least some data that is stored in the mobile terminal. ~~terminal,~~

~~wherein initiation of the method requires inputting a personal identification code at a location separate from the mobile terminal,~~

~~wherein the step of securing the stored data includes destroying at least part of the stored data after uploading the at least part of the stored data from the mobile terminal, and~~

~~wherein the guard message employs synchronization markup language device management if another program of the mobile terminal employs synchronization markup language device management, and otherwise the guard message either employs a smart message implemented as a bearer-independent object or employs wireless access protocol push messaging~~.

5. (Currently Amended) The method of <u>claim 4</u> ~~claim 1~~, wherein the personal identification code is different from a code used to operate the mobile terminal, and wherein initiation of the method also requires inputting a mobile terminal identifier.

6. (Original) The method of claim 5, wherein the personal identification code and the code used to operate the mobile terminal are both user-selected.

7. (Currently Amended) The method of <u>claim 4</u> ~~claim 1~~, wherein the user provides the personal identification code to an attendant, and the attendant then sends the guard message.

8. (Currently Amended) The method of <u>claim 4</u> ~~claim 1~~, wherein the guard message is sent repeatedly until an acknowledgment is received, or is sent when the mobile terminal is detected to be connected to a network, or both.

9. (Original) The method of claim 8, wherein the acknowledgment includes information about where the mobile terminal is located.

10. (Currently Amended) The method of <u>claim 4</u> ~~claim 1~~, wherein at least some of the stored data is encrypted prior to the uploading, after the receiving of the guard message.

11. CANCEL

12. (Currently Amended) A computer readable medium encoded with a software data structure sufficient for performing the method of claim 4 ~~claim 1~~.

13. CANCEL.

14. (Currently Amended) The ~~mobile terminal of claim 13~~ apparatus of claim 26, wherein the guard message employs a smart message implemented as a bearer-independent object, or employs wireless access protocol push messaging.

15. (Currently Amended) The ~~mobile terminal of claim 13~~ apparatus of claim 26, wherein the guard message employs synchronization markup language device management.

16. CANCEL

17. (Currently Amended) The ~~mobile terminal of claim 13~~ apparatus of claim 26, wherein the personal identification code is different from a code used to operate the mobile terminal, and wherein transmission of the guard message also requires inputting a mobile terminal identifier.

18. (Original) The mobile terminal of claim 17, wherein the personal identification code and the code used to operate the mobile terminal are both user-selected.

19. CANCEL.

20. CANCEL.

21. (Currently Amended) The ~~mobile terminal of claim 13~~ apparatus of claim 27, wherein the acknowledgment includes information about where the mobile terminal is located.

22. CANCEL

23. CANCEL

24. CANCEL.

25. CANCEL.

26. (New) Apparatus comprising:

a receiver device configured to receive a personal identification code of a mobile terminal that has been lost, stolen, or misplaced;

a database configured to reveal whether the mobile terminal corresponding to the personal identification code has a device management feature supporting synchronization markup language; and

a messaging device configured to compose and send a guard message to the mobile terminal;

wherein the messaging device is configured to employ a synchronization markup language if the mobile terminal has the device management feature,

wherein the messaging device instead is configured to employ a smart message implemented as a bearer-independent object or employs wireless access protocol push messaging, if the mobile terminal lacks the device management feature,

wherein the guard message contains instructions for the mobile terminal to lock at least one communication capability of the mobile terminal, and secure at least some data that is stored in the mobile terminal.

27. (New) The apparatus of claim 26, wherein the messaging device is further configured to send the guard message repeatedly until an acknowledgment is received.

28. (New) Apparatus comprising:

means for receiving a personal identification code of a mobile terminal that has been lost, stolen, or misplaced;

means for revealing whether the mobile terminal corresponding to the personal identification code has a device management feature supporting synchronization markup language; and

means for composing and sending a guard message to the mobile terminal;

wherein the guard message employs a synchronization markup language if the mobile terminal has the device management feature,

wherein the guard message instead employs a smart message implemented as a bearer-independent object or employs wireless access protocol push messaging, if the mobile terminal lacks the device management feature,

wherein the guard message contains instructions for the mobile terminal to lock at least one communication capability of the mobile terminal, and secure at least some data that is stored in the mobile terminal.

29. (New) The apparatus of claim 28, wherein the messaging device is further configured to send the guard message repeatedly until an acknowledgment is received.